Adaptive Beam Management for Secure mmWave Communications using Software-Defined Radios

Adrian Baron-Hyppolite*, Jefferson V. F. Abreu*, Joao F. Santos*, Luiz A. DaSilva*, and Jacek Kibiłda*
*Commonwealth Cyber Initiative, Virginia Tech, USA, E-mail: {adrianb, jeffersonva, joaosantos, ldasilva, jkibilda}@vt.edu

***Abstract*—mmWave systems leverage beamforming to generate narrow, high-powered beams for overcoming the increased path loss in the mmWave spectrum. These beams are spatially confined, making mmWave links more resilient to eavesdropping and jamming attacks. However, the mmWave radios locate each other and establish communication by exhaustively probing all possible angular directions, increasing the mmWave radios susceptibility to attacks. In this demonstration, we showcase a secure beam management solution where our mmWave radios apply an adaptive beam management procedure that avoids probing the directions of potential attackers. We employ a Reinforcement Learning agent to control the probing and dynamically restrict sweeps to a subset of beams in the mmWave radios' codebook to avoid the locations of potential attackers based on a proposed metric that quantifies the beam sweeping secrecy capacity over a pre-defined area.**

I. Introduction

To overcome the increased path loss, Millimeter-Wave (mmWave) systems leverage beamforming over large antenna arrays for generating narrow, high-powered beams. The spatially confined nature of these beams makes mmWave links more resilient to different types of attackers, e.g., eavesdroppers and jammers. However, mmWave radios require an Initial Access (IA) procedure to locate each other and determine the best Transmitter (Tx) and Receiver (Rx) beams for communication [1]. As part of the conventional IA, the mmWave radios perform an exhaustive beam sweeping, transmitting/receiving reference symbols to/from all combinations of angular directions in their codebooks [2]. Unfortunately, this procedure leads to sequential transmissions/receptions in a wide range of directions, which can reveal the location of the mmWave radios and lead to exploitation by eavesdroppers and jammers [3].

Most research efforts on IA for mmWave communications focus on its efficiency, e.g., [1], [2]. Few works, however, investigate security considerations related to IA and the relationship between its efficacy and increased exposure to attacks against mmWave communications [4]. In that spirit, the work of [5] proposed an approach to quantify the amount of information that can be securely transmitted over a single beam toward the direction of attackers while preserving the link quality between legitimate mmWave radios. However, the proposed technique does not factor in the beam sweeping, making it unsuitable for IA procedures employed in real systems.

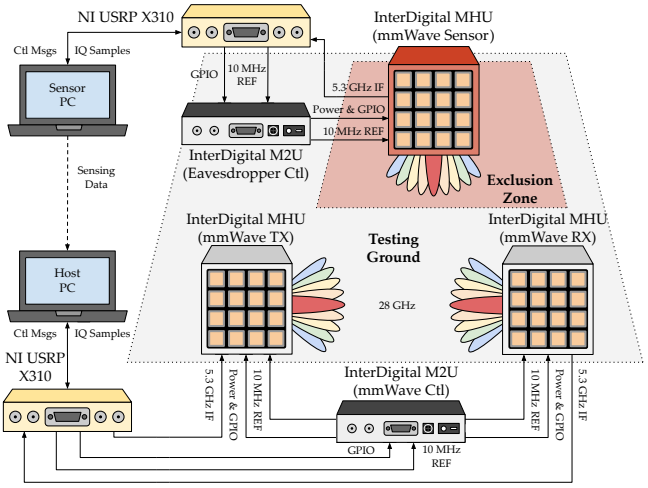

Fig. 1. Shows the equipment setup with three mmWave nodes. The Tx and Rx perform adaptive beam management to avoid the exclusion zone marked in red that contains the Rx sensor that measures the emissions.

In this demo, we showcase the first adaptive beam management solution for secure mmWave communications by optimizing beam sweeping in real time to prevent unwanted transmissions toward the location of potential attackers while preserving the performance of the communication link. To achieve this, we propose a Covert Beam-Sweep Pressure (CBSP) metric, based on the work of [5], which quantifies the secrecy capacity during the beam sweeping. Then, we design a Deep Reinforcement Learning (DRL) agent to perform adaptive beam management of the IA procedure, creating more restrictive custom sweeps using a subset of beams around arbitrary directions to avoid exclusion zones, according to the CBSP. The demonstration will showcase how our platform can dynamically adapt to arbitrary exclusion zones and generate custom beam USRPsweeps, securing mmWave communications.

II. Demo Design and Architecture

Fig. 1 shows our demonstration which will consist of a pair of Master Head Units (MHUs) representing the Tx and Rx antennas performing IA in proximity to an exclusion zone, which may contain a potential attacker; this attacker sensor is the third MHU located in the exclusion zone in Fig. 1. The MHUs are controlled by the MHU to USRPs (M2Us) units, which receive control signals from the Universal Software Radio Peripheral (USRP). Through the use

of our adaptive beam management solution, the mmWave radios will dynamically customize their beam sweeping space to determine the best Tx and Rx beams for communication, while avoiding transmitting/receiving towards the direction of the exclusion zone. An additional movable mmWave radio used as a sensor captures the Recieved Signal Strength (RSS) to exhibit how our system adapts to the changes in the environment as we adjust the location and size of the exclusion zone.

Our demo leverages mmWave equipment provided by InterDigital and resources from the CCI xG Testbed, which include: 3x MHU mmWave front-ends, 2x M2U mmWave controllers, 2x USRP X310 Software-Defined Radios (SDRs), and 2x host computers. Each MHU contains an 8×8 phased array antenna with a predefined codebook of 63 beams on a 9×7 grid that can be dynamically selected by controlling the M2U using its GPIO port. The MHU up/down-converts signals with bandwidth up to 200 MHz from/to Intermediate Frequency (IF) 5.3 GHz to/from the 28 GHz band, which allows the units to interface with the SDRs. We implemented our adaptive beam management solution on top of STAMINA, an out-of-tree GNU Radio module developed in our previous work to enable experimentation on IA procedures [6]. In the next section, we describe the operation of our adaptive beam management solution, introduce the CBSP metric, and detail our DRL agent for controlling the IA procedure.

III. Adaptive Beam Management

The development of the CBSP is motivated by the need to quantify the communication link security during beam-sweeping without pinpointing an attacker's location. The CBSP metric extends the secrecy pressure proposed in [5] by quantifying the loss of secrecy during the beam sweeping. zzFormally, CBSP is the difference between the capacity of the legitimate mmWave link and the mean capacity of the adversary link over an exclusion zone averaged over the applied codebook, as it measures the quantity of information transmitted, it is expressed in bits per second. We refer the reader to [5] for additional background information.

We utilize CBSP to design a custom agent to make decisions and perform an adaptive beam management of the IA procedure. Due to the dynamic nature of the mobile environment, e.g., user mobility or temporal blockages, which may affect the Tx-Rx beam alignment, we decided to employ a Reinforcement Learning (RL) approach to form effective policies that can adjust to these dynamics. For this implementation, we chose DRL composed of 4 linear layers connected by three ReLU activation layers because it can incorporate additional features, such as the previous best beam ID or the direction of the exclusion zone, resulting in more effective policy designs [7]. The DRL agent's objective is to select a beam-sweeping action that will maximize the reward based on the CBSP metric.

To verify the CBSP metric and experimentally validate our approach, we placed the legitimate Tx and Rx mmWave radios 11 feet apart, with an exclusion zone of a four-by-six-foot box set 4 ft to the right of the Rx mmWave radio. We considered three sweep spaces of different sizes: a 3×3 (9 beams), a 5×5 (25 beams), and an exhaustive beam sweep over the entire codebook of 9×7 (63 beams). Fig. 2 shows the results of our measurements. As expected, the more-restrictive 3×3 sweep space centered on the direction of the Rx produces the highest CBSP, indicating more information can be transmitted securely away from the exclusion zone. If the Tx and Rx are well-aligned, the smaller codebook size is preferable because the transmission directions are more restricted compared to the other larger codebooks.

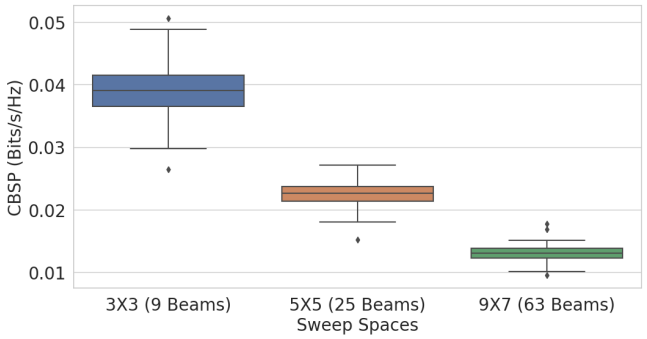

Fig. 2. The graph shows the CBSP values for three different sweep spaces captured on the CCI xG Testbed, with boxes indicating high and low quartiles of results collected and bars indicating outliers.

IV. Acknowledgement

The research leading to this paper received support from the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit: www.cyberinitiative.org. In addition, we would like to thank InterDigital for providing us with their mmWave equipment.

References

[1] T. S. Cousik *et al.*, "Fast Initial Access with Deep Learning for Beam Prediction in 5G mmWave Networks," in *IEEE Military Communications Conference*, 2021, pp. 664–669.

[2] J. Zhang *et al.*, "Beam Alignment and Tracking for Millimeter Wave Communications via Bandit Learning," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5519–5533, 2020.

[3] Y. Zeng and R. Zhang, "Wireless Information Surveillance via Proactive Eavesdropping with Spoofing Relay," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1449–1461, 2016.

[4] Z. Xing *et al.*, "Covert Millimeter Wave Communications Based on Beam Sweeping," *IEEE Communications Letters*, vol. 27, no. 5, pp. 1287–1291, 2023.

[5] L. Mucchi *et al.*, "A New Metric for Measuring the Security of an Environment: The Secrecy Pressure," *IEEE Transactions on Wireless Communications (TWC)*, vol. 16, no. 5, pp. 3416–3430, 2017.

[6] J. F. Santos *et al.*, "STAMINA: Implementation and Evaluation of Software-Defined Millimeter Wave Initial Access," in *IEEE International Conference on Communications (ICC)*, Rome, Italy, May 2023.

[7] N. Narengerile *et al.*, "Deep Reinforcement Learning-Based Beam Training for Spatially Consistent Millimeter Wave Channels," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 579–584.